

# Kolmogorov complexity version of Slepian-Wolf coding

Marius Zimand \*

## Abstract

Alice and Bob are given two correlated  $n$ -bit strings  $x_1$  and, respectively,  $x_2$ , which they want to losslessly compress and send to Zack. They can either collaborate by sharing their strings, or work separately. We show that there is no disadvantage in the second scenario: Alice and Bob, without knowing the other party's string, can achieve almost optimal compression in the sense of Kolmogorov complexity. Furthermore, compression takes polynomial time and can be made at any combination of lengths that satisfy some necessary conditions (modulo additive polylog terms). More precisely, there exist probabilistic algorithms  $E_1, E_2$ , and  $D$ , with  $E_1$  and  $E_2$  running in polynomial time, having the following behavior: if  $n_1, n_2$  are two integers satisfying  $n_1 + n_2 \geq C(x_1, x_2), n_1 \geq C(x_1 | x_2), n_2 \geq C(x_2 | x_1)$ , then for  $i \in \{1, 2\}$ ,  $E_i$  on input  $x_i$  and  $n_i$  outputs a string of length  $n_i + \text{polylog } n$  such that  $D$  on input  $E_1(x_1), E_2(x_2)$  reconstructs  $(x_1, x_2)$  with high probability (where  $C(x)$  denotes the plain Kolmogorov complexity of  $x$ , and  $C(x | y)$  is the complexity of  $x$  conditioned by  $y$ ). Our main result is more general, as it deals with the compression of any constant number of correlated strings. It is an analog in the framework of algorithmic information theory of the classic Slepian-Wolf Theorem, a fundamental result in network information theory, in which  $x_1$  and  $x_2$  are realizations of two discrete random variables formed by drawing independently  $n$  times from a joint distribution. Also, in the classical result, the decompressor needs to know the joint distribution of the sources. In our result no type of independence is assumed and the decompressor does not have any apriori information about the sources that are compressed, and it still is the case that distributed compression is on a par with centralized compression.

## 1 Introduction

The Slepian-Wolf Theorem [SW73] is the analog of the Shannon's Source Coding theorem for the case of distributed correlated sources. It characterizes the compression rates for such sources. To illustrate the theorem, let us consider a data transmission scheme with two senders, Alice and Bob, and one receiver, Zack. Alice has as input an  $n$ -bit string  $x$ , Bob has an  $n$ -bit string  $y$ . Alice uses the encoding function  $E_1 : \{0, 1\}^n \rightarrow \{0, 1\}^{n_1}$  to compress her  $n$ -bit string to length  $n_1$ , and sends  $E_1(x)$  to Zack. Bob, separately, uses the encoding function  $E_2 : \{0, 1\}^n \rightarrow \{0, 1\}^{n_2}$  to compress his  $n$ -bit string to length  $n_2$  and sends  $E_2(y)$  to Zack. We assume that the communication channels Alice  $\leftrightarrow$  Zack and Bob  $\leftrightarrow$  Zack are noise-free, and that there is no communication between Alice and Bob. Zack is using a decoding function  $D$  and the common goal of all parties is that  $D(E_1(x), E_2(y)) = (x, y)$ , for all  $x, y$  in the domain of interest (which is defined by the actual model or by the application). In a randomized setting, we allow the previous equality to fail with some small error probability  $\varepsilon$ . Of course, Alice can send the entire  $x$  and Bob can send

---

\*Department of Computer and Information Sciences, Towson University, Baltimore, MD.  
<http://triton.towson.edu/~mzimand>

the entire  $y$ , but this seems to be wasteful if  $x$  and  $y$  are correlated. We are interested to find what values can  $n_1$  and  $n_2$  take so that the goal is achieved.

The Slepian-Wolf theorem takes the standard stance in information theory which assumes that  $x$  and  $y$  are realizations of some random variables  $X$  and, respectively,  $Y$ . Furthermore, as it is common in information theory,  $(X, Y)$  are assumed to be 2-Discrete Memoryless Sources (2-DMS), which means that  $X = (X_1, \dots, X_n), Y = (Y_1, \dots, Y_n)$ , where the  $X_i$ 's are i.i.d. Bernoulli random variables, the  $Y_i$ 's are also i.i.d. Bernoulli random variables, and each  $(X_i, Y_i)$  is drawn according to a joint distribution  $p(b_1, b_2)$ . In other words,  $(X, Y)$  consists of  $n$  independent draws from a joint distributions on pair of bits. Given the joint distribution  $p(b_1, b_2)$  and  $X$  and  $Y$  of the specified type, the problem amounts to finding the set of values  $n_1$  and  $n_2$  such that there exists  $E_1, E_2$  and  $D$  as above with  $D(E_1(X), E_2(Y)) = (X, Y)$  with probability converging to 1 as  $n$  grows. In information theory parlance, we want to determine the set of achievable transmission rates. By the Source Coding Theorem, it is not difficult to see that it is necessary that  $n_1 \geq H(X | Y), n_2 \geq H(Y | X)$  and  $n_1 + n_2 \geq H(X, Y)$ , where  $H$  is the Shannon entropy function. The Slepian-Wolf theorem states that these relations are essentially sufficient, in the sense that any  $(n_1, n_2)$  satisfying strictly the above three inequalities is a pair of achievable rates, if  $n$  is sufficiently large ("strictly" means that " $>$ " replaces " $\geq$ "; see, for example, [CT06] for the exact statement).

What is surprising is that these optimal achievable rates can be realized with Alice and Bob doing their encoding separately. For example if  $H(X) = n, H(Y) = n$ , and  $H(X, Y) = 1.5n$ , then any pair  $(n_1, n_2)$ , with  $n_1 > 0.75n, n_2 > 0.75n$ , is a pair of achievable rates, which means that Alice can compress her  $n$ -bit realization of  $X$  to approximately  $0.75n$  bits, without knowing Bob's realization of  $Y$ , and Bob can do the same. They cannot do better even if they collaborate!

The Slepian-Wolf theorem completely characterizes the set of achievable rates for distributed lossless compression for the case of 2-DMS, and the result actually holds for an arbitrary number of senders (Theorem 15.4.2, [CT06]). However, the following issues affect the applicability of the theorem:

1. The type of correlations between  $X$  and  $Y$  given by the 2-DMS model is rather simple. In many applications the  $(X_i, Y_i)_i$  quantify some stochastic process at different times  $i$  and it is not realistic to assume independence between the values at different  $i$ 's. The Slepian-Wolf theorem has been extended for sources that are stationary and ergodic [Cov75], but these also capture relatively simple correlations.
2. The theorem does not guarantee that the protocol succeeds w.h.p. on all realizations  $x$  and  $y$  of  $X$  and  $Y$ . In fact, in the current proofs (as far as we know), there are some  $(x, y)$ , in which the protocol always fails.
3. The encoding and the decoding procedures in the current proofs are inefficient and assume that the senders and the receiver share a public random string of exponential length.

The first two issues are inherent to the information-theoretical model. Distributed correlated sources can be alternatively studied using algorithmic information theory, also known as Kolmogorov complexity, which does not have this shortcoming. One remarkable result in this framework is Muchnik's theorem [Muc02] which states that there exist algorithms  $E$  and  $D$  such that for all  $n$  and for all  $n$ -bit strings  $x$  and  $y$ ,  $E$  on input  $x$ ,  $C(x | y)$  and  $O(\log n)$  help bits outputs a string  $p$  and  $D$  on input  $p$ ,  $y$ , and  $O(\log n)$  help bits reconstructs  $x$  (we recall that  $C(u | v)$  is the Kolmogorov complexity of  $u$  conditioned by  $v$ , i.e., the length of a shortest program that

computes  $u$  given  $v$ ). Muchnik’s theorem relates to the asymmetric version of the above distributed transmission problem in which only Alice compresses her  $x$  while Bob sends the entire  $y$  (or, in an equivalent scenario, Zack already knows  $y$ ). It says that, given  $C(x | y)$ , Alice can compute from her string  $x$  and only  $O(\log n)$  additional help bits a string  $p$  of almost optimal length such that Zack using  $p$ ,  $y$  and  $O(\log n)$  help bits can reconstruct  $x$ . Muchnik’s theorem has been strengthened in several ways. Romashchenko [Rom05] has extended Muchnik’s theorem to the general (i.e., non-asymmetric) case. His result is valid for any constant number of senders, but, for simplicity, we present it for the case of two senders: For any two  $n$ -bit strings  $x$  and  $y$  and any two numbers  $n_1$  and  $n_2$  such that  $n_1 \geq C(x | y)$ ,  $n_2 \geq C(y | x)$  and  $n_1 + n_2 \geq C(x, y)$ , there exist two strings  $p_1$  and  $p_2$  such that  $|p_1| = n_1 + O(\log n)$ ,  $|p_2| = n_2 + O(\log n)$ ,  $C(p_1 | x) = O(\log n)$ ,  $C(p_2 | y) = O(\log n)$  and  $C(x, y | p_1, p_2) = O(\log n)$ . In words, for any  $n_1$  and  $n_2$  satisfying the necessary conditions, Alice can compress  $x$  to a string  $p_1$  of length just slightly larger than  $n_1$ , and Bob can compress  $y$  to a string  $p_2$  of length just slightly larger than  $n_2$  such that Zack can reconstruct  $(x, y)$  from  $(p_1, p_2)$ , provided all the parties use a few help bits. These results raise the following questions: (a) can the help bits be eliminated?<sup>1</sup>, and (b) is it possible to implement the protocol efficiently, i.e., in polynomial time? Bauwens et al. [BMVZ13] have obtained a version of Muchnik’s theorem with polynomial-time compression, but in which the help bits are still present. In fact, their result is stronger in that the compression procedure on input  $x$  outputs a polynomial-size list of strings guaranteed to contain a short program for  $x$  given  $y$ . This is called list approximation. Note that using  $O(\log n)$  help bits, the decoding procedure can pick the right element from the list, re-obtaining Muchnik’s theorem. The gain is that this decoding procedure halts even with incorrect help bits, even though the result may not be the desired  $x$ . Teutsch [Teu14] and Zimand [Zim14] have improved the result in [BMVZ13] in the “list-approximability” direction. Next, Bauwens and Zimand [BZ14] have eliminated the help bits in Muchnik’s theorem, at the cost of introducing a small error probability. Their result can be reformulated as follows.<sup>2</sup>

**Theorem 1.1** ([BZ14]). *There exist algorithms  $E$  and  $D$  such that  $E$  runs in probabilistic polynomial-time, and for all  $n$ -bit strings  $x$  and  $y$  and for every rational number  $\delta > 0$ ,*

1.  *$E$  on input  $x, 1/\delta$ , and  $C(x | y)$  outputs a string  $p$  of length  $C(x | y) + O(\log^2(n/\delta))$ , and*
2.  *$D$  on input  $p$  and  $y$  outputs  $x$  with probability  $1 - \delta$ .*

Thus in the asymmetric case, Alice can compress her input string in polynomial-time to length which is close to optimal in the sense of Kolmogorov complexity (closeness is within a polylog additive term). The decoding algorithm does not run in polynomial time and this is unavoidable if compression is done at this level of optimality because there exist so called deep strings (these are strings that have short descriptions, but their decompression from short description takes longer than, say, polynomial time). The procedures  $E$  and  $D$  are *promise* algorithms, because they require an additional integer as input and their behavior is guaranteed to be correct only as long as that integer is equal to  $C(x | y)$ . This also appears unavoidable,

---

<sup>1</sup>In Muchnik’s theorem, Alice computes a short program  $p$  such that  $U(p, y) = x$  from  $x$ ,  $C(x | y)$  and  $O(\log n)$  help bits, where  $U$  is the universal Turing machine underlying Kolmogorov complexity. One can hope to eliminate the  $O(\log n)$  help bits (as we ask in question (a)), but not the  $C(x | y)$  component. This is not possible even when  $y$  is the empty string. Indeed, it is known that for some strings  $x$ , the computation from  $x$  of  $C(x)$ , and therefore also the computation of a short program  $p$  for  $x$ , requires that some information of size  $\log |x| - O(1)$  bits is available [BS14, Gács74].

<sup>2</sup>In Theorem 3.2 in [BZ14],  $y$  is the empty string, but the proof works without modifications for any  $y$ .

because any pair  $E$  and  $D$  as above reveals  $C(x | y)$  (or at least a good approximation of it), which is uncomputable. Therefore, for compression at optimal length, it seems that  $C(x | y)$  needs to be known apriori.

In this paper, we prove the analog of Theorem 1.1 for the general non-asymmetric case, i.e., the case in which the number of senders is an arbitrary constant and all senders can compress their inputs. For simplicity, let us consider again the case with two senders, Alice and Bob, and one receiver, Zack. Alice and Bob are using probabilistic encoding algorithms  $E_1$ , and respectively  $E_2$ , Zack is using the decoding algorithm  $D$ , and they want that for all  $n$ , and for all  $n$ -bit strings  $x$  and  $y$ ,  $D(E_1(x), E_2(y)) = (x, y)$  with probability  $1 - \varepsilon$ . We denote  $|E_1(x)|$ , the length of  $x$ 's encoding, and  $|E_2(y)|$ , the length of  $y$ 's encoding. How large can these lengths be? By counting arguments, one can see that

$$\begin{aligned} |E_1(x)| &\geq C(x | y) + \log(1 - \varepsilon) - O(1) \\ |E_2(y)| &\geq C(y | x) + \log(1 - \varepsilon) - O(1) \\ |E_1(x)| + |E_2(y)| &\geq C(x, y) + \log(1 - \varepsilon) - O(1). \end{aligned}$$

Our result implies that the above requirements are also sufficient, except for a small overhead of polylog size. Namely, for any two integers  $n_1$  and  $n_2$  such that  $n_1 \geq C(x | y)$ ,  $n_2 \geq C(y | x)$  and  $n_1 + n_2 \geq C(x, y)$ , it is possible to achieve  $|E_1(x)| \leq n_1 + O(\log^3(n/\varepsilon))$ ,  $|E_2(y)| \leq n_2 + O(\log^3(n/\varepsilon))$ . Moreover  $E_1$  and  $E_2$  are polynomial-time probabilistic algorithms. If we do not insist on  $E_1$  and  $E_2$  running in polynomial time, the overhead can be reduced to  $O(\log(n/\varepsilon))$ .

For the general case, we need to introduce some notation. Let  $\ell$  be the number of senders. For any integers  $i$  and  $j$ , the set  $\{1, 2, \dots, i\}$  is denoted  $[i]$ , and the set  $\{i, i+1, \dots, j\}$  is denoted  $[i..j]$  (if  $i > j$ , this set is empty). If we have an  $i$  tuple of strings  $(x_1, \dots, x_i)$ , and  $V = \{i_1, i_2, \dots, i_k\} \subseteq [i]$ , then the  $k$ -tuple  $(x_{i_1}, x_{i_2}, \dots, x_{i_k})$  is denoted  $x_V$ .

**Theorem 1.2. (Main Result)** *There exists algorithms  $E_1, \dots, E_\ell$  and  $D$  and a function  $\alpha(n) = \log^{O(1)} n$  such that  $E_1, \dots, E_\ell$  are probabilistic polynomial-time algorithms, and for every  $n$ , for every  $\ell$ -tuple of integers  $(n_1, \dots, n_\ell)$ , and for every  $\ell$ -tuple of  $n$ -bit strings  $(x_1, \dots, x_\ell)$  if*

$$C(x_V | x_{[\ell]-V}) \leq \sum_{i \in V} n_i, \text{ for all } V \subseteq [\ell], \quad (1)$$

then

- (a) For all  $i \in [\ell]$ ,  $E_i$  on input  $x_i$  and  $n_i$  outputs a string  $p_i$  of length at most  $n_i + \alpha(n)$ ,
- (b)  $D$  on input  $(p_1, \dots, p_\ell)$  outputs  $(x_1, \dots, x_\ell)$  with probability  $1 - 1/n$ .

#### Comments

- The constraints (1) are necessary up to negligible terms. For example, if there are  $\ell = 3$  senders, having, respectively, the  $n$ -bit strings  $x_1, x_2$  and  $x_3$ , and they compress them, respectively, to lengths  $n_1, n_2$  and  $n_3$  and  $D(E_1(x_1), E_2(x_2), E_3(x_3)) = (x_1, x_2, x_3)$  with probability 0.99, then it is necessary that  $n_1 \geq C(x_1 | x_2, x_3) - O(1)$ ,  $n_2 \geq C(x_2 | x_1, x_3) - O(1)$ ,  $n_3 \geq C(x_3 | x_1, x_2) - O(1)$ ,  $n_1 + n_2 \geq C(x_1, x_2 | x_3) - O(1)$ ,  $n_1 + n_3 \geq C(x_1, x_3 | x_2) - O(1)$ ,  $n_2 + n_3 \geq C(x_2, x_3 | x_1) - O(1)$  and  $n_1 + n_2 + n_3 \geq C(x_1, x_2, x_3) - O(1)$ .

- Compared to Romashchenko's result from [Rom05], we have eliminated the help bits, and thus our encoding and decoding is effective. Moreover, encoding is done in polynomial time (however, as in Theorem 1.1 and for the same reason, decoding cannot be done in polynomial

time). The cost is that the encoding procedure is probabilistic and thus there is a small error probability. The proof of Theorem 1.2 is inspired from Romashchenko’s approach, but the technical elements are quite different.

- An interesting implication of the classic Slepian-Wolf Theorem is that distributed compression of correlated sources can be as good as centralized compression. In the classic theorem the sources are *independent* copies of a pair of jointly distributed random variables, and, in principle, the independence should be helpful for distributed compression (for instance, in the limit case when the sources are fully independent, clearly, it does not matter if compression is distributed or centralized). In Theorem 1.2 there is no assumption of independence, and it is still the case that distributed compression is on a par with centralized compression.

- In the classical Slepian-Wolf theorem, (a) the compression procedures need to know the compression lengths  $n_i$  (which collectively satisfy the necessary conditions analogous to (1)), and (b) the decompression procedure needs to know the joint distribution of the sources that are compressed. In Theorem 1.2, there is no requirement for decompression, i.e., we have eliminated (b).

Theorem 1.2 is interesting even for the case of a single source compression (i.e.,  $\ell = 1$ ). It is known that any algorithm that on input  $x$  and  $n_1 = C(x)$  outputs a shortest program for  $x$  runs in time larger than any computable function [BZ14]. Bauwens and Zimand (see Theorem 1.1) have shown that if we use randomization, one can find a short program for  $x$  in polynomial time, starting with input  $(x, n_1 = C(x))$ . Thus, computing a short program for  $x$  from  $x$  and  $C(x)$  is an interesting example of a task that probabilistically can be done in polynomial time, but deterministically requires time larger than any computable function. However the requirement that  $C(x)$  is known exactly is quite strong and unlikely to hold in applications. The following corollary, which is just Theorem 1.2 with  $\ell = 1$ , shows that in fact it is sufficient to have an upper bound  $n_1 \geq C(x)$ . This solves an open question from [TZ16].

**Corollary 1.3.** *There exists algorithms  $E$  and  $D$  such that  $E$  is a probabilistic polynomial-time algorithm, and for every  $n$ , for every  $n$ -bit string  $x$ , every positive rational number  $\delta > 0$ , and for every integer  $n_1 \geq C(x)$ ,*

- (a)  *$E$  on input  $x$  and  $1/\delta$  and  $n_1$  outputs a string  $p$  of length at most  $n_1 + O(\log^3(n/\delta))$ ,*
- (b)  *$D$  on input  $p$  outputs  $x$  with probability  $1 - \delta$ .*

## 2 Proof of Theorem 1.2

### 2.1 Combinatorial tool: graphs with the rich owner property

The key tool in the proof is a certain type of bipartite graph, which we call graphs with the rich owner property. Similar graphs, bearing the same name, were used in [BZ14], but the graphs in this paper have a stronger property. We recall that in a bipartite graph, the nodes are partitioned in two sets,  $L$  (the left nodes) and  $R$  (the right nodes), and all edges connect a left node to a right node. We allow multiple edges between two nodes. In all the graphs in this paper, all the left nodes have the same degree, called the left degree. Specifically, we use bipartite graphs  $G$  with  $L = \{0, 1\}^n$ ,  $R = \{0, 1\}^m$  and with left degree  $D = 2^d$ . We label the edges outgoing from  $x \in L$  with strings  $z \in \{0, 1\}^d$ . We typically work with a family of graphs indexed on  $n$  and such a family of graphs is *constructible* if there is an algorithm that on input  $(x, z)$ , where



$x \in L$  and  $z \in \{0, 1\}^d$ , outputs the  $z$ -th neighbor of  $x$ . Some of the graphs also depend on a rational  $0 < \delta < 1$ . A constructible family of graphs is *explicit* if the above algorithm runs in time  $\text{poly}(n, 1/\delta)$ .

We now introduce informally the notions of a *rich owner* and of a *graph with the rich owner property*. Let  $B \subseteq L$ . The  $B$ -degree of a right node is the number of its neighbors that are in  $B$ . Roughly speaking a left node is a rich owner with respect to  $B$ , if most of its right neighbors are “well-behaved,” in the sense that their  $B$ -degree is not much larger than  $|B| \cdot D/|R|$ , the average right degree when the left side is restricted to  $B$ . One particularly interesting case, which is used many times in this paper, is when most of the neighbors of a left  $x$  have  $B$ -degree 1, i.e., when  $x$  “owns” most of its right neighbors. A graph has the rich owner property if, for all  $B \subseteq L$ , most of the left nodes in  $B$  are rich owners with respect to  $B$ . In the formal definition, we replace the average right degree with an arbitrary value, but since in applications, this value is approximately equal to the average right degree, the above intuition should be helpful.

The precise definition of a  $(k, \delta)$ -rich owner with respect to  $B$  is as follows. There are two regimes of interest depending on how large is the size of  $B$ .

**Definition 2.1.** *Let  $G$  be a bipartite graph as above and let  $B$  be a subset of  $L$ . We say that  $x \in B$  is a  $(k, \delta)$ -rich owner with respect to  $B$  if the following holds:*

- small regime case: *If  $|B| \leq 2^k$ , then at least  $1 - \delta$  fraction of  $x$ 's neighbors have  $B$ -degree equal to 1, that is they are not shared with any other nodes in  $B$ . We also say that  $x \in B$  owns  $y$  with respect to  $B$  if  $y$  is a neighbor of  $x$  and the  $B$ -degree of  $y$  is 1.*
- large regime case: *If  $|B| > 2^k$ , then at least a  $1 - \delta$  fraction of  $x$ 's neighbors have  $B$ -degree at most  $(2/\delta^2)|B| \cdot D/2^k$ .*

*If  $x$  is not a  $(k, \delta)$ -rich owner with respect to  $B$ , then it is said to be a  $(k, \delta)$ -poor owner with respect to  $B$ .*

**Definition 2.2.** *A bipartite graph  $G = (L = \{0, 1\}^n, R = \{0, 1\}^m, E \subseteq L \times R)$  has the  $(k, \delta)$ -rich owner property if for every set  $B \subseteq L$  all nodes in  $B$ , except at most  $\delta|B|$  of them, are  $(k, \delta)$ -rich owners with respect to  $B$ .*

There are several notions in the literature which are related to our Definition 2.2, the main difference being that they require some non-congestion property similar to rich ownership to hold only for some subsets  $B$ . Reingold and Raz [RR99] define *extractor-condenser pairs*, in which only subsets  $B$  with size approximately  $2^k$  matter. As already mentioned, Bauwens and Zimand [BZ14] use a type of graph also called graphs with the rich owner property, which are close to the extractor-codenser pairs from [RR99]. Capalbo et al. [CRVW02] construct *lossless expanders*, which only consider the subsets  $B$  in the small regime case. In our application, we need to consider subsets  $B \subseteq L$  of *any* size and this lead to Definition 2.2, and the distinction between the small regime case and the large regime case.

The following theorem provides the type of graph that we use. The proof relies on the extractor from [RRV99] and uses a combination of techniques from [RR99], [CRVW02], and [BZ14]. It is presented in Section 4.

**Theorem 2.3.** *For every natural numbers  $n$  and  $k$  and for every real number  $\delta \in (0, 1]$ , there exists an explicit bipartite graph  $G = (L, R, E \subseteq L \times R)$  that has the  $(k, \delta)$ -rich property with the following parameters:*

- (I)  $L = \{0, 1\}^n$ ,

$$(II) \ R = \{0, 1\}^{k+\gamma(n/\delta)},$$

$$(III) \ \text{left degree } D = 2^{\gamma(n/\delta)},$$

where  $\gamma(n) = O(\log^3(n/\delta))$ .

## 2.2 Proof overview

For this proof sketch, we consider the case with  $\ell = 2$  senders, which have input strings  $x_1$  and, respectively,  $x_2$ . By hypothesis, the compression lengths  $n_1$  and  $n_2$  satisfy

$$n_1 \geq C(x_1 | x_2), n_2 \geq C(x_2 | x_1), n_1 + n_2 \geq C(x_1, x_2).$$

The two senders use graphs  $G_1$  and, respectively,  $G_2$ , with the  $(n_1, \delta)$  and, respectively,  $(n_2, \delta)$ -rich owner property and with  $\delta = 1/n^2$ , obtained from Theorem 2.3. The left nodes in both graphs are the set of  $n$ -bit strings, the right nodes in  $G_1$  are the binary strings of length  $n_1 + \gamma(n/\delta)$ , and the right nodes in  $G_2$  are the binary strings of length  $n_2 + \gamma(n/\delta)$ . Sender 1 picks  $p_1$ , a random neighbor of  $x_1$  (viewed as a left node) in  $G_1$ , and sender 2 picks  $p_2$ , a random neighbor of  $x_2$  (viewed as a left node) in  $G_2$ .

We need to explain how the receiver can reconstruct  $x_1$  and  $x_2$  from  $p_1$  and  $p_2$ . Most of the statements below hold with probability  $1 - O(\delta)$ . For conciseness, when this is clear, we omit mentioning this fact. We first assume that the decompression procedure knows  $C(x_1), C(x_2)$  and  $C(x_1, x_2)$  (this is usually called the complexity profile of  $x_1$  and  $x_2$ ). We will see later how to eliminate this assumption.

The first case to analyze is when  $C(x_2) \leq n_2$ . Then  $x_2$  can be constructed as follows. Let  $B = \{x \mid C(x) \leq C(x_2)\}$ . This is a subset of the left nodes in  $G_2$ , that contains  $x_2$ , and is in the *small regime case* (because  $|B| \leq 2^{C(x_2)} \leq 2^{n_2}$ ). The set of poor owners in  $G_2$  w.r.t.  $B$  has size at most  $\delta \cdot |B| = 2^{C(x_2) - \log(1/\delta)}$ . Since the set of poor owners w.r.t.  $B$  can be effectively enumerated given  $C(x_2)$ , we derive that every poor owner has complexity less than  $C(x_2)$ . So,  $x_2$  is a rich owner, which implies that with probability  $1 - \delta$ ,  $x_2$  does not share  $p_2$  with any other nodes in  $B$ . It follows that  $x_2$  can be constructed from  $p_2$  by enumerating  $B$  till we encounter a neighbor of  $p_2$ . As we have seen, with probability  $1 - \delta$ , this neighbor is  $x_2$ . Next, we take  $B = \{x'_1 \mid C(x'_1 | x_2) \leq C(x_1 | x_2)\}$ , and in a similar way we show that  $B$  is in the *small regime case* in  $G_1$ , and  $x_1$  is a rich owner w.r.t.  $B$ . Therefore, with probability  $1 - \delta$ ,  $x_1$  owns  $p_1$ . Thus, if we enumerate  $B$  till we encounter a neighbor of  $p_1$ , we obtain  $x_1$ .

The other case is when  $C(x_2) > n_2$ . We can show that with high probability,

$$C(p_2) =^* n_2, \tag{2}$$

where  $=^*$  means that the equality holds up to poly-logarithmic terms; we use  $\leq^*$  and  $\geq^*$  in a similar way. For that, again we consider  $B = \{x \mid C(x) \leq C(x_2)\}$ . This is a subset of the left nodes of  $G_2$  that is now in the *large regime case*. In the same way as above,  $x_2$  is a rich owner in  $G_2$  w.r.t.  $B$ , which implies that with probability  $1 - \delta$ , it shares  $p_2$  with at most  $(2/\delta^2)|B|D/2^{n_2} = 2^{C(x_2) - n_2 + \text{poly}(\log n)}$  other nodes in  $B$ . Taking into account that  $B$  can be enumerated given  $C(x_2)$ , it follows that  $x_2$  can be constructed from  $p_2$ ,  $C(x_2)$ , and  $x_2$ 's rank among  $p_2$ 's neighbors in  $B$ , which implies that  $C(x_2) \leq^* C(p_2) + (C(x_2) - n_2)$ . So,  $C(p_2) \geq^* n_2$ . Since the length of  $p_2$  is  $=^* n_2$ , we derive that  $C(p_2) =^* n_2$ .

The next observation is that, given  $p_2, x_1$  and  $C(x_2 | x_1)$ , the receiver can construct  $x_2$ . At this moment, the receiver does not have  $x_1$ , so actually  $x_2$  will be constructed later, after the

receiver has  $x_1$ . However, the observation is helpful even at this stage. Let us first see why the observation is true. Consider  $B = \{x'_2 \mid C(x'_2 \mid x_1) \leq C(x_2 \mid x_1)\}$ . This is a subset of left nodes in  $G_2$  that contains  $x_2$ , and is in the *small regime case* (because  $|B| \leq 2^{C(x_2 \mid x_1)} \leq 2^{n_2}$ ). Similarly to the argument used earlier,  $x_2$  is a rich owner w.r.t.  $B$ . So,  $x_2$  owns  $p_2$  w.r.t.  $B$ , which implies that  $x_2$  can be obtained by enumerating the elements of  $B$  till we encounter one that is a neighbor of  $p_2$ .

The observation implies that  $C(x_2, x_1) \leq^* C(p_2, x_1)$ . Since it also holds that  $C(p_2, x_1) \leq^* C(x_2, x_1)$  (because  $p_2$  can be obtained from  $x_2$  and its index among  $x_2$ 's neighbors in  $G_2$ , which takes poly log  $n$  bits to describe), we have

$$C(x_2, x_1) =^* C(p_2, x_1). \quad (3)$$

Then, by (2) and (3),

$$C(x_1 \mid p_2) =^* C(x_1, p_2) - C(p_2) =^* C(x_1, x_2) - n_2, \quad (4)$$

where the first  $=^*$  follows from the chain rule. The last estimation, allows the receiver to reconstruct  $x_1$  from  $p_1$  and  $p_2$ . For that, consider  $B = \{x'_1 \mid C(x'_1 \mid p_2) \leq C(x_1, x_2) - n_2\}$ . Our estimation (4) of  $C(x_1 \mid p_2)$  implies that  $x_1$  is in  $B$ . Next, by the same argument as above, the poor owners in  $G_1$  have complexity conditioned by  $p_2$  less than  $C(x_1, x_2) - n_2$ , and this implies that  $x_1$  is not a poor owner. Since  $C(x_1, x_2) - n_2 \leq (n_1 + n_2) - n_2 = n_1$ ,  $B$  is in the *small regime case*. This implies that with high probability  $x_1$  owns  $p_1$  in  $G_1$  w.r.t.  $B$ . So, if we enumerate  $B$  till we encounter a neighbor of  $p_1$ , we obtain  $x_1$ .

With  $x_1$  in hand, the receiver constructs  $x_2$ , using the earlier observation.

**Decompression without knowledge of the input's complexity profile.** As promised, we show how to eliminate the assumption that the decompressor  $D$  knows  $C(x_1), C(x_2), C(x_1, x_2)$ . The idea is to let  $D$  run the above procedure for all possibilities of  $C(x_1), C(x_2), C(x_1, x_2)$  and use hashing to isolate the correct run (or some run that produces the same output). Since  $x_1$  and  $x_2$  are  $n$ -bit strings, there are  $O(n^3)$  possibilities for the triplet  $(C(x_1), C(x_2), C(x_1, x_2))$  and hashing will add only  $O(\log n)$  bits. For hashing we use the following result. Alternatively, it is possible to use the almost  $\delta$ -universal function of Naor and Naor [NN93], or Krawczyk [Kra94].

**Lemma 2.4** ([BZ14]). *Let  $x_1, x_2, \dots, x_s$  be distinct  $n$ -bit strings, which we view in some canonical way as integers  $< 2^{n+1}$ .*

*Let  $q_i$  be the  $i$ -th prime number and let  $L = \{q_1, \dots, q_t\}$ , where  $t = (1/\delta) \cdot s \cdot n$ .*

*For every  $i \leq s$ , for  $(1 - \delta)$  fraction of  $q$  in  $L$ , the value of  $x_i \bmod q$  is unique in the sequence  $(x_1 \bmod q, x_2 \bmod q, \dots, x_s \bmod q)$ .*

For  $i = 1, 2$ , Sender  $i$  who has input  $x_i$  will send in addition to  $p_i$  (a random neighbor of  $x_i$  in  $G_i$ , as we have seen above), also  $(q_i, x_i \bmod q_i)$  where  $q_i$  is a prime number chosen at random from the first  $t$  prime numbers, where  $t = (1/\delta) \cdot s \cdot n$ , and  $s = (n + O(1))^3$  is an upper bound for the number of all triplets  $(C(u), C(v), C(u, v))$  where  $u$  and  $v$  are  $n$ -bit strings. The decompressor runs *in parallel* the procedure presented above for all  $s$  guesses for  $(C(x_1), C(x_2), C(x_1, x_2))$  and halts when the first of the parallel runs outputs  $x'_1, x'_2$  with  $x'_1 \bmod q_1 = x_1 \bmod q_1$  and  $x'_2 \bmod q_2 = x_2 \bmod q_2$ . Note that some of the parallel runs may not halt, but the run corresponding to the correct guess of  $(C(x_1), C(x_2), C(x_1, x_2))$  halts and yields, as we have seen,  $(x_1, x_2)$  with probability  $1 - O(\delta)$ . By Lemma 2.4, the probability that a run halts with  $x'_1 \neq x_1$  or  $x'_2 \neq x_2$  but  $x'_1 \bmod q_1 = x_1 \bmod q_1$  and  $x'_2 \bmod q_2 = x_2 \bmod q_2$  is at most  $\delta$ . Consequently, this procedure



reconstructs correctly  $(x_1, x_2)$  with probability  $1 - O(\delta)$ . Since the  $t$ -th prime number is bounded by  $t \log t$  and can be found in time polynomial in  $t$ , the length of each of the compressed strings increases with only  $O(\log t) = O(\log(n/\delta))$  bits, and the running time of compression is still polynomial.

If the number of senders is  $\ell > 2$ , several technical complications arise. In the case  $\ell = 2$ , sketched above, the decoding algorithm needs to have  $C(x_1), C(x_2)$  and  $C(x_1, x_2)$  to be able to enumerate the various sets  $B$ . Recall that we assume that the receiver knows the complexity profile of the input strings, and therefore, the decoding algorithm has these values. When  $\ell \geq 3$ , the various sets  $B$  are defined in term of complexities containing certain combinations of the input strings  $x_i$ 's, and of the randomly picked right neighbors,  $p_j$ 's. To give just one example, the complexity  $C(x_{[k]}, p_{[k+1..\ell]})$  is required at some point. The decoding algorithm needs to obtain, with high probability, good approximations of such complexities from the complexity profile of the input strings (see Lemma 2.7). Another technical aspect is that the approximation slacks (hidden above in the notation  $=^*, \leq^*, \geq^*$ , and also those arising in the estimations of the complexities of “combined” tuples of  $x_i$ 's and  $p_j$ 's) cannot be ignored as we did in this proof sketch. To handle this, senders use graphs with decreasing  $\delta$ 's (i.e.,  $\delta_\ell > \delta_{\ell-1} > \dots > \delta_1$ ) and increasing overhead in the length of the right neighbors. More precisely, sender  $k$  (for every  $k \in [\ell]$ ), uses a graph  $G_k$  with the  $\delta_k$ -rich neighbor property, in which the right nodes have length  $n_k + \gamma(n/\delta_k) + \eta_k(n)$ , where the additional  $\eta_k(n)$  is needed to handle the effect of approximations. The overhead  $\gamma(n/\delta_k) + \eta_k(n)$  is bounded by  $(\log n)^{O_\ell(1)}$ , where  $O_\ell(1)$  denotes a constant that depends on  $\ell$ . In spite of these technicalities, the core ideas of the proof are those presented in the above sketch.

### 2.3 Parameters

We fix  $n$ , the length of the input strings  $x_1, \dots, x_\ell$ .

We use a constant  $c$  that will take a large enough value so that the estimations done in this proof are all valid. The construction uses parameters  $(\delta_\ell, \delta_{\ell-1}, \dots, \delta_1)$ ,  $(\gamma_\ell, \gamma_{\ell-1}, \dots, \gamma_1)$ ,  $(\eta_\ell, \eta_{\ell-1}, \dots, \eta_1)$  and  $(\hat{\delta}_\ell, \hat{\delta}_{\ell-1}, \dots, \hat{\delta}_1)$  that are all functions of  $n$  and are defined as follows.

- For all  $k \in [\ell]$ ,  $\gamma_k$  is defined in terms of  $\delta_k$ , according to the relation given in Theorem 2.3:  $\gamma_k = O(\log^3(n/\delta_k))$ . We also define  $\gamma_{\ell+1} = 0$ .

- The parameters  $\delta_k$  are defined recursively in descending order as follows:  $1/\delta_\ell = c \cdot n$ , and then  $1/\delta_k = 2^{17\gamma_{k+1}}$ , for  $k = \ell - 1, \dots, 1$ . Note that for all  $k \in [\ell - 1]$ ,  $(1/\delta_k) = 2^{(\log n)^{O_\ell(1)}}$ ,  $\gamma_k = O(\log^3 n \cdot \gamma_{k+1}^3)$  and  $\gamma_k = (\log n)^{O_\ell(1)}$ , where  $O_\ell(1)$  denotes a constant that depends on  $\ell$ . We will use the fact that for any constant  $a$ , the following inequalities hold provided  $n$  is large enough:

$$\gamma_k \geq a(\gamma_{k+1} + \log(1/\delta_k^2) + \log n), \quad (5)$$

and

$$\log(1/\delta_k) > 16\gamma_{k+1} + a \log n. \quad (6)$$

- We next define for all  $k \in [\ell]$ ,

$$\eta_k = 2\gamma_k + \log(2/\delta_k^2). \quad (7)$$

Note that for all  $k$ ,  $\eta_k = (\log n)^{O_\ell(1)}$ .

- We denote  $\hat{n}_k = n_k + \eta_k + 1$ .

• The sequence  $\hat{\delta}_\ell, \hat{\delta}_{\ell-1}, \dots, \hat{\delta}_1$  is defined recursively (in descending order) as follows:  $\hat{\delta}_\ell = \delta_\ell$  and

$$\hat{\delta}_k = 2\hat{\delta}_{k+1} + \delta_k.$$

It can be checked that  $(1/\hat{\delta}_k) = 2^{(\log n)^{O_\ell(1)}}$

## 2.4 Handling the input complexity profile

As we did in Section 2.2, Proof overview, we first assume that the decompressor  $D$  knows the complexity profile of the input strings  $x_1, \dots, x_\ell$ , which is the tuple  $(C(x_V) \mid V \subseteq [\ell], V \neq \emptyset)$ . This assumption can be eliminated in the same way as we did in the proof overview.

## 2.5 Encoding

Each sender  $k$ ,  $k \in [\ell]$ , considers the graph  $G_k$  promised by Theorem 2.3, with  $L = \{0, 1\}^n$ ,  $R = \{0, 1\}^{\hat{n}_k + \gamma_k}$  that has the  $(\hat{n}_k, \delta_k)$ -rich owner property. Thus left nodes are  $n$ -bit strings and in this way the input string  $x_k$  is a left node in  $G_k$ . Sender  $k$  picks  $p_k$  uniformly at random among the right neighbors of  $x_k$  in the graph  $G_k$ , and sends  $p_k$  to the receiver. The length of  $p_k$  is  $\hat{n}_k + \gamma_k = n_k + (\log n)^{O_\ell(1)}$ .

## 2.6 Decoding

We first state some technical lemmas that play an important role in the decoding procedure. They are proved in Section 3. The first two lemmas estimate how the complexity of  $p_k$  is related to the complexity of  $x_k$ , for  $k \in [\ell]$ . There are two regimes to analyze, depending on whether the complexity of  $x_k$  is low or high. We analyze the respective complexities conditioned by some string  $b$ , which for now is an arbitrary string, but later when we apply these lemmas for  $p_k$  and  $x_k$ ,  $b$  will be instantiated with the previous inputs  $x_{[k-1]}$  and the nodes  $p_{[k+1..\ell]}$ .

**Lemma 2.5.** (low complexity case) *Let  $b$  be an arbitrary string and suppose  $C(x_k \mid b) \leq n_k + \eta_k$ .*

- (I) *There exists an algorithm that on input  $b, p_k$  and  $C(x_k \mid b)$  outputs  $x_k$  with probability  $1 - \delta_k$  (over the random choice of  $p_k$ ).*
- (II) *With probability  $1 - \delta_k$ ,  $|C(p_k, b) - C(x_k, b)| \leq \gamma_k + O(\log n) = (\log n)^{O_\ell(1)}$ .*

**Lemma 2.6.** (high complexity case) *Let  $b$  be an arbitrary string and suppose  $C(x_k \mid b) > n_k$ .*

- (I) *There exists an algorithm that on input  $b, p_k$ ,  $C(x_k \mid b)$  and some string  $b'$  of length  $|b'| \leq \max(0, C(x_k \mid b) - (n_k + \eta_k - \gamma_k - \log(2/\delta_k^2)))$ , outputs  $x_k$  with probability  $1 - \delta_k$  (over the random choice of  $p_k$ ).*
- (II) *With probability  $1 - \delta_k$ ,  $|C(p_k, b) - (C(b) + n_k + \eta_k)| \leq \gamma_k + \eta_k + \log(2/\delta_k^2) + O(\log n) = (\log n)^{O_\ell(1)}$  and  $C(p_k \mid b) \geq n_k + \eta_k - \gamma_k - \log(2/\delta_k^2) - O(\log n) = n_k - (\log n)^{O_\ell(1)}$ .*

The decoding procedure needs good estimations of the complexities of the form  $C(x_k \mid x_{[k-1]}, p_{[k+1..\ell]})$ . The following lemma shows that it is possible to effectively approximate them with precision  $(\log n)^{O_\ell(1)}$ . The inductive proof requires the approximation of more general complexities of the form  $C(x_V, p_{[k+1..\ell]})$  for all  $V \in \mathcal{P}([k])$  and for all  $k \in [\ell]$ .

**Lemma 2.7.** *There is an algorithm with the following behaviour:*

*For all  $k \leq \ell$ , the algorithm on input  $(p_{k+1}, \dots, p_\ell)$ ,  $V \in \mathcal{P}([k])$ , and  $C(x_W)$  for all non-empty  $W \subseteq [\ell]$ , outputs an integer  $A(x_V, p_{k+1}, \dots, p_\ell)$  such that with probability  $1 - \hat{\delta}_k$ ,*

$$|C(x_V, p_{[k+1..\ell]}) - A(x_V, p_{[k+1..\ell]})| \leq 4\gamma_{k+1} = (\log n)^{O_\ell(1)}.$$

The next lemma shows that the constraints (1) remain roughly valid if we replace the left nodes  $x_{k+1}, \dots, x_\ell$  with the corresponding right nodes  $p_{k+1}, \dots, p_\ell$ .

**Lemma 2.8.** *For all  $k \leq \ell$ , for all non-empty  $V \subseteq [k]$ , the following inequality holds with probability  $1 - \hat{\delta}_k$ :*

$$C(x_V \mid x_{[k]-V}, p_{[k+1..\ell]}) \leq \sum_{j \in V} n_j + O(\ell - k) \cdot \log n$$

### Decoding algorithm

Some of the estimations below hold with error probability bounded by  $\hat{\delta}_k$  or  $\delta_k$ , for various  $k \in [\ell]$ , and all these values are bounded by  $\delta_\ell = 1/(c \cdot n)$  (the probability is on the random choices of  $p_1, \dots, p_\ell$ ). There are  $O_\ell(1)$  “bad” events when the estimations are violated. By taking  $c$  sufficiently large, the union of all “bad events” has probability at most  $1/n$ . The following arguments are done conditioned on the event that none of the “bad” events happened.

First, using the algorithm from Lemma 2.7, the values  $A(x_k \mid x_{[k-1]}, p_{[k+1..\ell]})$  are calculated by the formula

$$A(x_k \mid x_{[k-1]}, p_{[k+1..\ell]}) = A(x_k, x_{[k-1]}, p_{[k+1..\ell]}) - A(x_{[k-1]}, p_{[k+1..\ell]}).$$

By the chain rule and the bounds on approximation error established in Lemma 2.7, it holds that

$$|C(x_k \mid x_{[k-1]}, p_{[k+1..\ell]}) - A(x_k \mid x_{[k-1]}, p_{[k+1..\ell]})| \leq 8\gamma_{k+1} + O(\log n). \quad (8)$$

The decoding algorithm reconstructs in order  $x_1, x_2, \dots, x_\ell$ .

**Step 1** (reconstruction of  $x_1$ ).

By Lemma 2.8,

$$C(x_1 \mid p_{[2..\ell]}) \leq n_1 + O(\ell - 2) \log n. \quad (9)$$

Consider the graph  $G_1 = (L, R, E \subseteq L \times R)$  used by sender 1.  $G_1$  has  $L = \{0, 1\}^n$ ,  $R = \{0, 1\}^{\hat{n}_1 + \gamma_1}$ , left degree  $D = 2^{\gamma_1}$ , and the  $(\hat{n}_1, \delta_1)$ -rich owner property. Consider the set

$$B = \{x \in \{0, 1\}^n \mid C(x \mid p_{[2..\ell]}) \leq A(x_1 \mid p_{[2..\ell]}) + 8\gamma_2 + O(\log n)\},$$

where the constant hidden in the  $O()$  is taken so that  $x_1$  is in  $B$  (keeping in mind the estimation (8) for  $k = 1$ ).

The subset of  $(\hat{n}_1, \delta_1)$ -poor owners w.r.t.  $B$  has size at most  $\delta_1 \cdot |B| \leq \delta_1 \cdot 2^{A(x_1 \mid p_{[2..\ell]}) + 8\gamma_2 + O(\log n)}$ . Note that the set of poor owners can be enumerated given  $p_{[2..\ell]}$ ,  $A(x_1 \mid p_{[2..\ell]})$ ,  $\hat{n}_1$ , and  $\delta_1$ . Given  $p_{[2..\ell]}$ ,  $A(x_1 \mid p_{[2..\ell]})$  can be computed from  $n$  and the complexity profile of the input strings (by Lemma 2.7). The integers  $\hat{n}_1$  and  $\delta_1$  can be computed from  $n$  and  $n_1$  and we can assume that

$n_1 \leq n$  (otherwise, sender 1 can simply send  $x_1$  uncompressed). It follows that if  $x$  is a poor owner, then

$$\begin{aligned}
C(x \mid p_{[2..\ell]}) &\stackrel{(a)}{\leq} \log(\delta_1 \cdot |B|) + O(\log n) \\
&\stackrel{(b)}{\leq} A(x_1 \mid p_{[2..\ell]}) + 8\gamma_2 - \log(1/\delta_1) + O(\log n) \\
&\stackrel{(c)}{\leq} C(x_1 \mid p_{[2..\ell]}) + 16\gamma_2 - \log(1/\delta_1) + O(\log n) \\
&\stackrel{(d)}{<} C(x_1 \mid p_{[2..\ell]}).
\end{aligned}$$

Transition (a) follows taking into account the above explanations and the fact that  $x$  is described by its index in the enumeration of poor owners, transition (b) uses the above bound for the number of poor owners, transition (c) follows from (8), and transition (d) follows from (6).

Therefore,  $x_1$  cannot be a poor owner, so it is a  $(\hat{n}_1, \delta_1)$ -rich owner in  $G_1$ . The size of  $B$  is bounded by  $2^{n_1 + \eta_1 + 1}$  because

$$\begin{aligned}
A(x_1 \mid p_{[2..\ell]}) + 8\gamma_2 + O(\log n) &\stackrel{(a)}{\leq} C(x_1 \mid p_{[2..\ell]}) + 16\gamma_2 + O(\log n) \\
&\stackrel{(b)}{\leq} n_1 + 16\gamma_2 + O(\ell - 2) \log n \\
&\stackrel{(c)}{<} n_1 + \eta_1 + 1 = \hat{n}_1.
\end{aligned}$$

Transition (a) follows from (8), transition (b) follows from (9), and transition (c) follows from (7) and (5).

Hence  $B$  is in the “small regime” case for the graph  $G_1$ . It follows that with probability  $1 - \delta_1$ ,  $x_1$  is the only node in  $B$  that is a neighbor of  $p_1$  in  $G_1$ . Therefore,  $x_1$  can be reconstructed as follows: Enumerate  $B$  till we encounter one element that is a left neighbor of  $p_1$  in  $G_1$  and output this element. By the above discussion, this procedure will output  $x_1$  with high probability.

**Step k** (we have already obtained  $x_1, \dots, x_{k-1}$  and now we reconstruct  $x_k$ ).

The argument is similar to the one in Step 1. By Lemma 2.8,  $C(x_k \mid x_{[k-1]}, p_{[k+1..\ell]}) \leq n_k + O(\ell - k) \log n$ . Consider the graph  $G_k = (L, R, E \subseteq L \times R)$  used by sender  $k$ .  $G_k$  has  $L = \{0, 1\}^n, R = \{0, 1\}^{\hat{n}_k + \gamma_k}$ , left degree  $D = 2^{\gamma_k}$ , and the  $(\hat{n}_k, \delta_k)$ -rich owner property. Consider the set

$$B = \{x \in \{0, 1\}^n \mid C(x \mid x_{[k-1]}, p_{[k+1..\ell]}) \leq A(x_k \mid x_{[k-1]}, p_{[k+1..\ell]}) + 8\gamma_{k+1} + O(\log n)\},$$

where the constant hidden in the  $O()$  is taken so that  $x_k$  is in  $B$  (keeping in mind the estimation (8)). Using a similar argument as in Step 1,  $x_k$  is a  $(\hat{n}_k, \delta_k)$ -rich owner w.r.t  $B$  in  $G_k$  and  $B$  is in the “small regime” case, because

$$\begin{aligned}
A(x_k \mid x_{[k-1]}, p_{[k+1..\ell]}) + 8\gamma_{k+1} + O(\log n) &\stackrel{(a)}{\leq} C(x_k \mid x_{[k-1]}, p_{[k+1..\ell]}) + 16\gamma_{k+1} + O(\log n) \\
&\stackrel{(b)}{\leq} n_k + 16\gamma_{k+1} + O(\ell - k) \log n \\
&\stackrel{(c)}{<} n_k + \eta_k + 1 = \hat{n}_k.
\end{aligned}$$

Transition (a) follows from (8), transition (b) follows from Lemma 2.8, and transition (c) follows from (7) and (5). Therefore, similarly to Step 1,  $x_k$  can be obtained from  $x_{[k-1]}, p_k$ , and  $p_{[k+1..\ell]}$ , because  $x_k$  owns  $p_k$  w.r.t.  $B$  in  $G_k$ , and  $B$  can be enumerated given  $x_{[k-1]}$ , and  $p_{[k+1..\ell]}$ .

### 3 Proofs of the technical lemmas

This section contains the proofs of Lemma 2.5, Lemma 2.6, Lemma 2.7, and Lemma 2.8.

**Proof of Lemma 2.5.** (i) The graph  $G_k = (L_k, R_k, E_k \subseteq L_k \times R_k)$ , used by sender  $k$  for doing the encoding is obtained by applying Theorem 2.3 with parameters  $n, k = n_k + \eta_k + 1 = \hat{n}_k$  and  $\delta_k$ , and thus has  $L_k = \{0, 1\}^n, R_k = \{0, 1\}^{\hat{n}_k + \gamma_k}$  and the  $(\hat{n}_k, \delta_k)$ -rich owner property. Let

$$B = \{x \in \{0, 1\}^n \mid C(x \mid b) \leq C(x_k \mid b)\}.$$

Note that  $B$ 's size is bounded by  $2^{C(x_k \mid b)+1}$  and, obviously,  $x_k \in B$ .

The subset of poor owners w.r.t.  $B$  has size at most  $\delta|B| \leq \delta_k \cdot 2^{C(x_k \mid b)+1}$  and can be enumerated given  $b$  and  $C(x_k \mid b)$ . It follows that if  $x$  is a poor owner w.r.t.  $B$ , then

$$\begin{aligned} C(x \mid b) &\leq C(x_k \mid b) + 1 - \log(1/\delta_k) + O(\log n) \\ &< C(x_k \mid b), \end{aligned}$$

where the second inequality holds because  $1/\delta_k \geq 1/\delta_\ell = cn$  and  $c$  is chosen to be a large enough constant. Consequently,  $x_k$  cannot be a poor owner, and therefore it is a  $(\hat{n}_k, \delta_k)$ -rich owner w.r.t.  $B$ . Since  $|B| \leq 2^{C(x_k \mid b)+1}$  and  $C(x_k \mid b) + 1 \leq n_k + \eta_k + 1 = \hat{n}_k$ , we are in the “small regime” case. By the property of graphs with the rich owner property in this regime of parameters, it follows that with probability  $(1 - \delta_k)$ ,  $x_k$  is the only node in  $B$  that is a neighbor of  $p_k$ . This leads to the following algorithm that constructs  $x_k$ , on input  $b, p_k$  and  $C(x_k \mid b)$ : Enumerate  $B$  till one of the enumerated nodes is a neighbor of  $p_k$ . As we have seen, with probability  $1 - \delta_k$ , this node is  $x_k$ .

(ii) It follows from (i) that, with probability  $1 - \delta_k$ ,

$$\begin{aligned} C(x_k, b) &\leq C(p_k, b) + 2\log C(x_k \mid b) + O(1) \\ &\leq C(p_k, b) + 2\log n + O(1). \end{aligned}$$

Since  $C(p_k, b) \leq C(x_k, b) + \gamma_k + O(\log n)$  (because  $p_k$  can be obtained from  $x_k$  and the index of the edge that links  $x_k$  and  $p_k$  among the edges going out from  $x_k$ ; next, we take into account that the left degree of  $G$  is  $2^{\gamma_k}$  and consequently the index requires  $\gamma_k$  bits), the conclusion follows.  $\square$

**Proof of Lemma 2.6.** There are two cases to analyze: *Case 1*:  $C(x_k \mid b) \in (n_k, n_k + \eta_k]$  and *Case 2*:  $C(x_k \mid b) > n_k + \eta_k$ .

In *Case 1*, the same estimations as in Lemma 2.5 hold, because we are still in the *small regime case*. Thus, we obtain

$$C(x_k \mid b) - 2\log n - O(1) \leq C(p_k \mid b) \leq C(x_k \mid b) + \gamma_k + O(\log n).$$

Using the fact that we are in Case 1, we can substitute  $C(x_k \mid b)$  and obtain

$$n_k + \eta_k - (\eta_k + O(\log n)) \leq C(p_k \mid b) < n_k + \eta_k + (\gamma_k + O(\log n)).$$

Using the chain rule, we obtain

$$C(b) + n_k + \eta_k - (\eta_k + O(\log n)) \leq C(p_k, b) < C(b) + n_k + \eta_k + (\gamma_k + O(\log n)),$$

which implies

$$|C(p_k, b) - (C(b) + n_k + \eta_k)| \leq \eta_k + \gamma_k + O(\log n). \quad (10)$$



We next analyze *Case 2*. For (i), as in Lemma 2.5, we note that  $x_k$  is a  $(\hat{n}_k, \delta_k)$ -rich owner w.r.t.  $B = \{x \in \{0, 1\}^n \mid C(x \mid b) \leq C(x_k \mid b)\}$ . We are now in the *large regime case* and it follows that with probability  $1 - \delta_k$ ,  $p_k$  has at most  $(2/\delta_k^2)|B|2^{\gamma_k}/2^{\hat{n}_k}$  neighbors in  $B$ , of which one is  $x_k$ . Note that

$$\frac{(2/\delta_k^2)|B|2^{\gamma_k}}{2^{\hat{n}_k}} \leq \frac{2^{C(x_k|b)+\gamma_k+\log(2/\delta_k^2)+1}}{2^{\hat{n}_k}} = 2^{C(x_k|b)-(n_k+\eta_k-\gamma_k-\log(2/\delta_k^2))}.$$

So,  $x_k$  can be constructed from  $b, p_k, C(x_k \mid b)$  and the index of  $x_k$  in an enumeration of  $p_k$ 's neighbors in  $B$ . This index is a string  $b'$  of length at most  $C(x_k \mid b) - (n_k + \eta_k - \gamma_k - \log(2/\delta_k^2))$ .

(ii) From part (i), with probability  $1 - \delta_k$ ,

$$C(x_k \mid b) \leq C(p_k \mid b) + (C(x_k \mid b) - (n_k + \eta_k - \gamma_k - \log(2/\delta_k^2))) + O(\log n).$$

Therefore,

$$C(p_k \mid b) \geq n_k + \eta_k - \gamma_k - \log(2/\delta_k^2) - O(\log n), \quad (11)$$

which proves the second inequality in (ii). Next,

$$\begin{aligned} C(p_k, b) &\stackrel{(a)}{\geq} C(b) + C(p_k \mid b) - O(\log n) \\ &\stackrel{(b)}{\geq} C(b) + n_k + \eta_k - \gamma_k - \log(2/\delta_k^2) - O(\log n). \end{aligned}$$

Transition (a) follows by the chain rule and transition (b) uses (11). In the other direction, we have the inequality

$$C(p_k, b) \leq C(b) + |p_k| + O(\log n) = C(b) + n_k + \eta_k + \gamma_k + O(\log n).$$

It follows that

$$|C(p_k, b) - (C(b) + n_k + \eta_k)| \leq \gamma_k + \log(2/\delta_k^2) + O(\log n). \quad (12)$$

Combining (10) with (12), the conclusion follows.  $\square$

**Proof of Lemma 2.7.** The computation is done iteratively in descending order for  $k = \ell, \ell - 1, \dots, 1$ .

At the first iteration  $k = \ell$ , there is nothing to compute because the values  $C(x_V)$  are given, and thus the algorithm simply takes  $A(x_V) = C(x_V)$  for all  $V \in \mathcal{P}([\ell])$ . Note that  $\gamma_{\ell+1} = 0$ .

Suppose we have performed the iterations  $\ell, \ell - 1, \dots, k$  and now we are at iteration  $k - 1$ .

So we have already computed  $A(x_{V'}, p_{[k+1..\ell]})$  for all non-empty  $V' \subseteq [k]$  and with probability  $1 - \hat{\delta}_{k+1}$ ,

$$|C(x_{V'}, p_{[k+1..\ell]}) - A(x_{V'}, p_{[k+1..\ell]})| \leq 2\gamma_{k+1}.$$

Let us fix a non-empty  $V \subseteq [k - 1]$ . We will define  $A(x_V, p_{[k+1..\ell]})$  (we do this below in equations (14) and (16)). For this, we want to approximate  $C(x_V, p_k, \dots, p_\ell)$  because the plan is to use either Lemma 2.5, (ii) or Lemma 2.6, (ii), with  $b \leftarrow (x_V, p_{[k+1..\ell]})$ . Which of the two lemmas is applicable depends on whether the complexity  $C(x_k \mid b)$  is low or high. Note that  $C(x_k \mid$

$b) = C(x_k, b) - C(b) \pm c \log n$  and at the previous iteration we have computed the approximations  $A(x_k, b)$  and  $A(b)$  for  $C(x_k, b)$  and respectively  $C(b)$ . Therefore we distinguish two cases.

**Case 1 (low complexity case).** Suppose  $A(x_{V \cup \{k\}}, p_{[k+1..\ell]}) - A(x_V, p_{[k+1..\ell]}) \leq n_k + 8\gamma_{k+1} + c \log n$ .

Note that with probability  $1 - \hat{\delta}_{k+1}$ ,

$$\begin{aligned}
C(x_k \mid x_V, p_{[k+1..\ell]}) & \\
&\stackrel{(a)}{\leq} C(x_V, x_k, p_{[k+1..\ell]}) - C(x_V, p_{[k+1..\ell]}) + c \log n \\
&\stackrel{(b)}{\leq} A(x_V, x_k, p_{[k+1..\ell]}) - A(x_V, p_{[k+1..\ell]}) + 8\gamma_{k+1} + c \log n \\
&\stackrel{(c)}{\leq} n_k + 16\gamma_{k+1} + 2c \log n \\
&\stackrel{(d)}{\leq} n_k + \eta_k.
\end{aligned}$$

Transition (a) follows by the chain rule, transition (b) uses the induction hypothesis, transition (c) uses the assumption that we are in Case 1, and transition (d) uses (7) and (5). By Lemma 2.5 (ii) (with  $b \leftarrow X_V, p_{[k+1..\ell]}$ ), with probability  $1 - \delta_k$ ,

$$|C(x_V, p_k, p_{[k+1..\ell]}) - C(x_V, x_k, p_{[k+1..\ell]})| \leq \gamma_k + c \log n. \quad (13)$$

So, we define

$$A(x_V, p_k, p_{[k+1..\ell]}) := A(x_V, x_k, p_{[k+1..\ell]}). \quad (14)$$

Then, with probability  $1 - 2\hat{\delta}_{k+1} - \delta_k = 1 - \hat{\delta}_k$ ,

$$\begin{aligned}
&|C(x_V, p_k, p_{[k+1..\ell]}) - A(x_V, p_k, p_{[k+1..\ell]})| \\
&\leq |C(x_V, p_k, p_{[k+1..\ell]}) - C(x_V, x_k, p_{[k+1..\ell]})| + |C(x_V, x_k, p_{[k+1..\ell]}) - A(x_V, p_k, p_{[k+1..\ell]})| \\
&\stackrel{(a)}{=} |C(x_V, p_k, p_{[k+1..\ell]}) - C(x_V, x_k, p_{[k+1..\ell]})| + |C(x_V, x_k, p_{[k+1..\ell]}) - A(x_V, x_k, p_{[k+1..\ell]})| \\
&\stackrel{(b)}{\leq} \gamma_k + c \log n + 4\gamma_{k+1} \\
&\stackrel{(c)}{\leq} 4\gamma_k.
\end{aligned}$$

Transition (a) follows by (14), transition (b) uses (13) and the induction hypothesis, and transition (c) uses (5).

**Case 2 (high complexity case).** Suppose  $A(x_{V \cup \{k\}}, p_{[k+1..\ell]}) - A(x_V, p_{[k+1..\ell]}) > n_k + 8\gamma_{k+1} + c \log n$ .

This time, with probability  $1 - 2\hat{\delta}_{k+1}$ ,

$$\begin{aligned}
C(x_k \mid x_V, p_{[k+1..\ell]}) & \\
&\stackrel{(a)}{\geq} C(x_{V \cup \{k\}}, p_{[k+1..\ell]}) - C(x_V, p_{[k+1..\ell]}) - c \log n \\
&\stackrel{(b)}{\geq} A(x_{V \cup \{k\}}, p_{[k+1..\ell]}) - A(x_V, p_{[k+1..\ell]}) - 8\gamma_{k+1} - c \log n \\
&\stackrel{(c)}{\geq} n_k.
\end{aligned}$$

Transition (a) follows by the chain rule, transition (b) uses the induction hypothesis, and transition (c) uses the assumption that we are in Case 2. By Lemma 2.6 (ii), with probability  $1 - \delta_k$ ,

$$|C(x_V, p_k, p_{[k+1..\ell]}) - (C(x_V, p_{[k+1..\ell]}) + n_k + \eta_k)| \leq \gamma_k + \eta_k + \log(2/\delta_k^2) + c \log n. \quad (15)$$

So, we define

$$A(x_V, p_k, p_{[k+1..\ell]}) := A(x_V, p_{[k+1..\ell]}) + n_k + \eta_k. \quad (16)$$

Then, with probability  $1 - 2\hat{\delta}_{k+1} - \delta_k \geq 1 - \hat{\delta}_k$ ,

$$\begin{aligned} & |C(x_V, p_k, p_{[k+1..\ell]}) - A(x_V, p_k, p_{[k+1..\ell]})| \\ & \leq |C(x_V, p_k, p_{[k+1..\ell]}) - (C(x_V, p_{[k+1..\ell]}) + n_k + \eta_k)| + \\ & \quad + |(C(x_V, p_{[k+1..\ell]}) + n_k + \eta_k) - A(x_V, p_k, p_{[k+1..\ell]})| \\ & \stackrel{(a)}{\leq} |C(x_V, p_k, p_{[k+1..\ell]}) - (C(x_V, p_{[k+1..\ell]}) + n_k + \eta_k)| + \\ & \quad + |(C(x_V, p_{[k+1..\ell]}) + n_k + \eta_k) - (A(x_V, p_{[k+1..\ell]}) + n_k + \eta_k)| \\ & \stackrel{(b)}{\leq} \gamma_k + \eta_k + \log(2/\delta_k^2) + c \log n + 4\gamma_{k+1} \\ & \stackrel{(c)}{=} \gamma_k + 2\gamma_k + 2\log(2/\delta_k^2) + c \log n + 4\gamma_{k+1} \\ & \stackrel{(d)}{\leq} 4\gamma_k. \end{aligned}$$

Transition (a) follows by (16), transition (b) uses (15) and the induction hypothesis, transition (c) uses (7), and transition (d) uses (5).  $\square$

**Proof of Lemma 2.8.** We do backward induction on  $k$ . The statement is true for  $k = \ell$ , by hypothesis. Suppose we have proven the statement for  $k + 1$ . We prove it for  $k$ . Let  $V \subseteq [k]$ .

**Case 1 (low complexity case).** Suppose  $C(x_{k+1} \mid x_{[k]-V}, p_{[k+2..\ell]}) \leq n_{k+1} + \eta_{k+1}$ .

We apply Lemma 2.5 for  $k + 1$  and  $b := x_{[k]-V}, p_{[k+2..\ell]}$ . We obtain that, with probability  $1 - \delta_{k+1}$ ,  $x_{k+1}$  can be constructed from  $p_{k+1}, b$  and  $C(x_{k+1} \mid b)$ .

Next,

$$\begin{aligned} C(x_V \mid x_{[k]-V}, p_{[k+1..\ell]}) & \stackrel{(a)}{\leq} C(x_V \mid x_{[k]-V}, x_{k+1}, p_{[k+2..\ell]}) + c \log n \\ & = C(x_V \mid x_{[k+1]-V}, p_{[k+2..\ell]}) + c \log n \\ & \stackrel{(b)}{\leq} \sum_{j \in V} n_j + O(\ell - k - 1) \cdot \log n + c \log n \\ & = \sum_{j \in V} n_j + O(\ell - k) \cdot \log n. \end{aligned}$$

Transition (a) holds by the above argument with probability  $1 - \delta_k$ , transition (b) holds by the induction hypothesis with probability  $1 - \hat{\delta}_{k+1}$ . Thus the entire chain of inequalities holds with probability  $1 - \hat{\delta}_{k+1} - \delta_{k+1} \geq 1 - \hat{\delta}_k$ .

**Case 2 (high complexity case).** Suppose  $C(x_{k+1} \mid x_{[k]-V}, p_{[k+2..\ell]}) > n_{k+1} + \eta_{k+1}$ .

Then, Lemma 2.6, used for  $k + 1$  and  $b := x_{[k]-V}, p_{[k+2..\ell]}$ , implies that with probability  $1 - \delta_{k+1}$ ,

$$C(p_{k+1} \mid x_{[k]-V}, p_{[k+2..\ell]}) \geq n_{k+1} + \eta_{k+1} - \gamma_{k+1} - \log(2/\delta_{k+1}^2) - c \log n. \quad (17)$$

Next,

$$\begin{aligned}
& C(x_V \mid x_{[k]-V}, p_{[k+1..\ell]}) \\
& \stackrel{(a)}{\leq} C(x_V, p_{k+1} \mid x_{[k]-V}, p_{[k+2..\ell]}) - C(p_{k+1} \mid x_{[k]-V}, p_{[k+2..\ell]}) + c \log n \\
& \stackrel{(b)}{\leq} C(x_V, p_{k+1} \mid x_{[k]-V}, p_{[k+2..\ell]}) - n_{k+1} - \eta_{k+1} + \gamma_{k+1} + \log(2/\delta_{k+1}^2) + 2c \log n \\
& \stackrel{(c)}{\leq} C(x_V, x_{k+1} \mid x_{[k]-V}, p_{[k+2..\ell]}) - n_{k+1} - \eta_{k+1} + \gamma_{k+1} + \log(2/\delta_{k+1}^2) + \gamma_{k+1} + 2c \log n \\
& \stackrel{(d)}{\leq} C(x_{V \cup \{k+1\}} \mid x_{[k+1]-V \cup \{k+1\}}, p_{[k+2..\ell]}) - n_{k+1} + 2c \log n \\
& \stackrel{(e)}{\leq} \left( \sum_{j \in V \cup \{k+1\}} n_j \right) + O(\ell - k - 1) \cdot \log n - n_{k+1} + 2c \log n \\
& = \sum_{j \in V} n_j + O(\ell - k) \cdot \log n.
\end{aligned}$$

Transition (a) follows by the chain rule, transition (b) follows from inequality (17) and holds with probability  $1 - \delta_{k+1}$ , transition (c) follows from the fact that  $p_{k+1}$  can be obtained from  $x_{k+1}$  and the index of the edge that connects  $x_{k+1}$  and  $p_{k+1}$  and this index needs  $\gamma_{k+1}$  bits, transition (d) holds due to (7). Inequality (e) holds with probability  $1 - \hat{\delta}_{k+1}$  by the induction hypothesis for  $k + 1$ . Taking into account transitions (a) and (e), the entire chain of inequalities holds with probability  $1 - \hat{\delta}_{k+1} - \delta_{k+1} \geq 1 - \hat{\delta}_k$ .  $\square$

## 4 Construction of graphs with the rich owner property

In this section we prove Theorem 2.3. The construction relies on the randomness extractor of Raz, Reingold, and Vadhan [RRV99]. We recall that a  $(k, \varepsilon)$  extractor is a function  $E : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  such that for any distribution  $X$  on  $\{0, 1\}^n$  with min-entropy  $H_\infty(X) \geq k$ ,  $E(X, U_d)$  is  $\varepsilon$ -close to  $U_m$ , where  $U_d$  ( $U_m$ ) is the uniform distribution on  $\{0, 1\}^d$  (respectively,  $\{0, 1\}^m$ ), i.e., for every  $A \subseteq R$ ,

$$\left| \text{Prob}[E(X, U_d) \in A] - \frac{|A|}{M} \right| < \varepsilon. \quad (18)$$

**Theorem 4.1** ([RRV99]). *There exists a family of functions  $E : \{0, 1\}^n \times \{0, 1\}^{d(n)} \rightarrow \{0, 1\}^{k(n)}$  such that*

- (1) *For every  $k' \leq k(n)$ , the prefix  $k'$  of  $E$  (i.e., the function obtained by computing  $E$  and retaining only the first  $k'$  bits of the output) is a  $(k', \varepsilon)$  extractor;*
- (2)  $d(n) = O(\log^2(n/\varepsilon(n)) \log n)$ .

Next we convert the extractor from Theorem 4.1 into a graph with the rich owner property. The method follows closely [BZ14]. We first establish several lemmas.

Let  $E : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  be a  $(k, \varepsilon)$  extractor, and let  $G_E = (L = \{0, 1\}^n, R = \{0, 1\}^m, E_G)$  be the corresponding bipartite graph, i.e., there is an edge  $(x, z) \in E_G$  iff there exists  $y$  such that  $E(x, y) = z$ . Let  $B \subseteq L$ . The  $B$ -degree of a node  $y$  (denoted  $\deg_B(y)$ ) is the number of  $y$ 's neighbors that are in  $B$ . Let  $D = 2^d$ .

A vertex  $y \in R$  is  $t$ -heavy for  $B$  if  $\deg_B(y) \geq t \cdot \frac{|B|2^d}{|R|}$  (otherwise  $y$  is  $t$ -light for  $B$ ).

Let  $A = \{y \in R \mid y \text{ is } t\text{-heavy for } B\}$ .

A vertex  $x \in B$  is  $\delta$ -bad for  $B$  if  $\deg_A(x)/\deg(x) \geq \delta$  (i.e., more than a  $\delta$  fraction of edges outgoing from  $x$  land in nodes that are  $t$ -heavy for  $B$ ).

**Lemma 4.2.** *For every bipartite graph  $G$ , for every  $B \subseteq L$ , for every  $t > 0$ ,  $|A| \leq \frac{1}{t}|R|$ .*

**Proof** The number of edges between  $B$  and  $A$  is at least  $|A| \cdot t \cdot \frac{|B| \cdot D}{|R|}$ . On the other hand, the total number of edges between  $B$  and  $R$  is  $|B| \cdot D$ . Thus,  $|A| \cdot t \cdot \frac{|B| \cdot D}{|R|} \leq |B| \cdot D$ , from which the conclusion follows.  $\square$

Let  $\delta$ -BAD be the set of vertices in  $B$  which are  $\delta$ -bad for  $B$ .

**Lemma 4.3.** *If  $|B| \geq 2^k$ , then  $\frac{|\delta\text{-BAD}|}{|B|} \leq \frac{1}{\delta} \left( \frac{1}{t} + \varepsilon \right)$ .*

**Proof** Let  $X$  be the distribution which is flat on  $B$  (i.e., it assigns equal probability mass to elements in  $B$ , and 0 probability mass to every element which is not in  $B$ ). Then,  $H_\infty(X) \geq k$ . Let  $\mu_E$  be the distribution induced by the extractor  $E$  on  $R$  when  $x$  is chosen according to distribution  $X$  and  $y$  is chosen uniformly at random in  $\{0, 1\}^d$ . Formally, for  $Z \subseteq R$ ,

$$\mu_E(Z) = \frac{|\{(x, y) \mid x \in B, y \in \{0, 1\}^d, E(x, y) \in Z\}|}{|B| \cdot D}.$$

Since  $E$  is  $(k, \varepsilon)$ -extractor,  $\mu_E(A) \leq \frac{|A|}{|R|} + \varepsilon \leq \frac{(1/t)|R|}{|R|} + \varepsilon = \frac{1}{t} + \varepsilon$ .

On the other hand,  $\mu_E(A) \geq \frac{|\delta\text{-BAD}| \cdot \delta D}{|B| \cdot D} = \frac{|\delta\text{-BAD}|}{|B|} \cdot \delta$ .

So,  $\frac{|\delta\text{-BAD}|}{|B|} \leq \frac{1}{\delta} \cdot \mu_E(A) \leq \frac{1}{\delta} \left( \frac{1}{t} + \varepsilon \right)$ .  $\square$

Now we describe the transformation of an extractor graph into a graph with the rich owner property. We use again the hashing technique provided by Lemma 2.4.

Let  $s$  be a positive integer and let  $\delta > 0$ . The following algorithm transforms  $G_1 = (L = \{0, 1\}^n, R_1 = \{0, 1\}^m, E_1)$ , a bipartite graph into another bipartite graph  $G$  as follows.

Let  $\ell = (1/\delta) \cdot s \cdot n$  and let  $q_1, q_2, \dots, q_\ell$  be the first  $\ell$  prime numbers. We construct the bipartite graph

$$G = (L = \{0, 1\}^n, R = \{q_1, \dots, q_\ell\} \times \{0, 1, \dots, q_\ell - 1\} \times R_1, E),$$

by adding for each  $(x, z)$  in  $E_1$  the edges

$$(x, (q_1, x \bmod q_1, z)), (x, (q_2, x \bmod q_2, z)), \dots, (x, (q_\ell, x \bmod q_\ell, z))$$

in  $E$  (one can think that each edge  $(x, z) \in G_1$  is split into  $\ell$  edges in  $G$ ).

**Lemma 4.4.** *Let  $G_1 = (L_1 = \{0, 1\}^n, R_1 = \{0, 1\}^k, E_1 \subseteq L_1 \times R_1)$  be the  $(k, \varepsilon)$ -extractor with left degree  $D_1 = 2^{d_1}$  from Theorem 4.1. Let  $\delta = (2\varepsilon)^{1/2}$  and let  $G = (L, R, E \subseteq L \times R)$  be constructed from  $G_1$  as above with  $s = (2/\delta^2) \cdot 2^{d_1}$ . Then:*



- (1)  $G$  has the  $(k, 2\delta)$ -rich owner property.
- (2)  $L = \{0, 1\}^n$
- (3)  $R$  can be taken to be  $\{0, 1\}^{3\log \ell} \times \{0, 1\}^k$ , where  $\ell = (1/\delta) \cdot s \cdot n$ .
- (4) The left degree of  $G$  is bounded by  $2^d \cdot \ell$ .
- (5) If  $G_1$  is explicit, then  $G$  is explicit.

**Proof** We analyze first the *small regime case*. Let  $B \subseteq L$  be a subset of size  $2^{k'} \leq 2^k$  (to simplify the notation we assume that the size of  $B$  is a power of two). We consider the graph  $G'_1$ , the  $k'$ -prefix of  $G_1$ , which means that  $G'_1$  is obtained from  $G_1$  by reducing the labels of the right nodes from their initial  $k$ -bit value to the prefix of length  $k'$ . By Theorem 4.1,  $G'_1$  is a  $(k', \varepsilon)$  extractor. By Lemma 4.3 (in which we take  $\varepsilon = \delta^2/2$  and  $t = 2/\delta^2$ ), there is a “bad” set  $\delta$ -BAD  $\subseteq B$  of size  $|\delta$ -BAD  $\leq \delta|B|$ , such that for all the “good” nodes  $x \in B - \delta$ -BAD, in  $G'_1$ , it holds that at least  $(1 - \delta)$  fraction of edges outgoing from  $x$  land in right nodes that are  $t$ -light for  $B$ , i.e., land in right nodes that have  $B$ -degree in  $G'_1$  at most  $(2/\delta^2) \cdot |B| \cdot D_1/|R'_1| = (2/\delta^2) \cdot (2^{k'+d_1-k'}) = s$ . The  $B$ -degree of a node in  $G_1$  can be at most the  $B$ -degree of its prefix in  $G'_1$ , and therefore the above holds in  $G_1$  as well.

Let us fix a “good” node  $x \in B - \delta$ -BAD. Suppose the multiset of  $x$ ’s neighbors in  $G_1$  is  $\{z_1, z_2, \dots, z_D\}$ . We write the neighbors of  $x$  in  $G$  in the following tabular form:

$$\begin{array}{cccc}
 (q_1, x \bmod q_1, z_1) & (q_2, x \bmod q_2, z_1) & \dots & (q_\ell, x \bmod q_\ell, z_1) \\
 (q_1, x \bmod q_1, z_2) & (q_2, x \bmod q_2, z_2) & \dots & (q_\ell, x \bmod q_\ell, z_2) \\
 \vdots & & & \\
 (q_1, x \bmod q_1, z_D) & (q_2, x \bmod q_2, z_D) & \dots & (q_\ell, x \bmod q_\ell, z_D)
 \end{array}$$

In at least a fraction of  $(1 - \delta)$  rows, the corresponding  $z_i$  has  $\deg_B(z_i) \leq s$  in  $G_1$ , so each node in such a row is shared by at most  $s$  elements of  $B$ , say  $x, x_2, \dots, x_s$ . In each such row, if we look at the components  $q_i, x \bmod q_i$  and take into account Lemma 2.4, we conclude that at least a fraction  $(1 - \delta)$  of the elements in the row have a unique neighbor in  $B$  (in  $G$ ). Thus, overall, at least a fraction of  $(1 - \delta)^2 > (1 - 2\delta)$  of the neighbors of  $x$  are unique. Since this holds for every  $x \in B - \delta$ -BAD and  $|B - \delta$ -BAD  $= |B| - |\delta$ -BAD  $\geq (1 - \delta)|B| > (1 - 2\delta)|B|$ , we are done.

Next, we analyze the *large regime case*. Let  $B \subseteq L$  be a subset of size  $2^{k'} > 2^k$ . By Lemma 4.3 (in which again we take  $\varepsilon = \delta^2/2$  and  $t = 2/\delta^2$ ), there is a “bad” set  $\delta$ -BAD  $\subseteq B$  of size  $|\delta$ -BAD  $\leq \delta|B|$ , such that for all the “good” nodes  $x \in B - \delta$ -BAD, in  $G_1$ , it holds that at least  $(1 - \delta)$  fraction of edges outgoing from  $x$  land in right nodes that are  $t$ -light for  $B$ , i.e., they are shared with at most  $(2/\delta^2) \cdot |B| \cdot D_1/|R| = (2/\delta^2) \cdot |B| \cdot D_1/2^k$  other nodes from  $B$ . The edge splitting operation can only reduce congestion, and the left degree increases from  $D_1$  to  $D = D_1 \cdot \ell$ . So, in  $G$  it holds that all the “good” nodes  $x \in B - \delta$ -BAD, have at least a  $(1 - \delta)$  fraction of edges outgoing from  $x$  that land in right nodes that are shared with at most  $(2/\delta^2) \cdot |B| \cdot D/2^k$  other nodes from  $B$ . Since  $|B - \delta$ -BAD  $= |B| - |\delta$ -BAD  $\geq (1 - \delta)|B| > (1 - 2\delta)|B|$ , we are done.

The parameters of  $G$  follow from its construction taking into account that  $q_\ell \leq \ell \log \ell$  and that the  $\ell$ ’s prime number can be found in time polynomial in  $\ell$ .  $\square$

The proof of Theorem 2.3 follows immediately from Lemma 4.4.

## 5 Acknowledgments

The author is grateful to Nikolay Vereshchagin and Alexander Shen for useful discussions. Sasha Shen suggested the idea that led to the elimination in the main result of the requirement that the inputs' complexity profile must be given to the decompression procedure. The author thanks his father, Rudy Zimand, for helping him with the Russian language in [Rom05] (an English version is now available [Rom16]).

## References

- [BMVZ13] B. Bauwens, A. Makhlin, N. Vereshchagin, and M. Zimand. Short lists with short programs in short time. In *Proceedings of 28th IEEE Conference on Computational Complexity, Stanford, California, USA*, 2013.
- [BS14] B. Bauwens and A. Shen. Complexity of complexity and maximal plain versus prefix-free Kolmogorov complexity. *Journal of Symbolic Logic*, 79(2):620–632, 2014.
- [BZ14] Bruno Bauwens and Marius Zimand. Linear list-approximation for short programs (or the power of a few random bits). In *IEEE 29th Conference on Computational Complexity, CCC 2014, Vancouver, BC, Canada, June 11-13, 2014*, pages 241–247. IEEE, 2014.
- [Cov75] Thomas M. Cover. A proof of the data compression theorem of Slepian and Wolf for ergodic sources (corresp.). *IEEE Transactions on Information Theory*, 21(2):226–228, 1975.
- [CRVW02] M. R. Capalbo, O. Reingold, S. P. Vadhan, and A. Wigderson. Randomness conductors and constant-degree lossless expanders. In John H. Reif, editor, *STOC*, pages 659–668. ACM, 2002.
- [CT06] Thomas M. Cover and Joy A. Thomas. *Elements of information theory* (2. ed.). Wiley, 2006.
- [Gác74] P. Gács. On the symmetry of algorithmic information. *Soviet Math. Dokl.*, 15:1477–1480, 1974.
- [Kra94] Hugo Krawczyk. LFSR-based hashing and authentication. In Yvo Desmedt, editor, *Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings*, volume 839 of *Lecture Notes in Computer Science*, pages 129–139. Springer, 1994.
- [Muc02] Andrei A. Muchnik. Conditional complexity and codes. *Theor. Comput. Sci.*, 271(1-2):97–109, 2002.
- [NN93] Joseph Naor and Moni Naor. Small-bias probability spaces: Efficient constructions and applications. *SIAM Journal on Computing*, 22(4):838–856, August 1993.
- [Rom05] A. Romashchenko. Complexity interpretation for the fork network coding. *Information Processes*, 5(1):20–28, 2005. In Russian. Available in English as [Rom16].

- [Rom16] Andrei Romashchenko. Coding in the fork network in the framework of Kolmogorov complexity. *CoRR*, abs/1602.02648, 2016.
- [RR99] Ran Raz and Omer Reingold. On recycling the randomness of states in space bounded computation. In Jeffrey Scott Vitter, Lawrence L. Larmore, and Frank Thomson Leighton, editors, *STOC*, pages 159–168. ACM, 1999.
- [RRV99] R. Raz, O. Reingold, and S. Vadhan. Extracting all the randomness and reducing the error in trevisan’s extractor. In *Proceedings of the 30th ACM Symposium on Theory of Computing*, pages 149–158. ACM Press, May 1999.
- [SW73] D. Slepian and J.K. Wolf. Noiseless coding of correlated information sources. *IEEE Transactions on Information Theory*, 19(4):471–480, 1973.
- [Teu14] Jason Teutsch. Short lists for shortest descriptions in short time. *Computational Complexity*, 23(4):565–583, 2014.
- [TZ16] Jason Teutsch and Marius Zimand. A brief on short descriptions. *SIGACT News*, 47(1):42–67, March 2016.
- [Zim14] Marius Zimand. Short lists with short programs in short time - A short proof. In Arnold Beckmann, Erzsébet Csuhaj-Varjú, and Klaus Meer, editors, *Language, Life, Limits - 10th Conference on Computability in Europe, CiE 2014, Budapest, Hungary, June 23-27, 2014. Proceedings*, volume 8493 of *Lecture Notes in Computer Science*, pages 403–408. Springer, 2014.